

RNO

ADMINISTRATIVE - INTERNAL USE ONLY

5 JUN 1975

MEMORANDUM FOR: Agency ADP Control Officers

SUBJECT : Classification of Computer Storage Media

1. With the proliferation of computer equipments and the expansion of computer operations throughout the Agency, the appropriate classification and marking of computer storage media is a matter of security concern. As a consequence, you are asked to bring to the attention of appropriate personnel under your cognizance portions of Headquarters [redacted] "Freedom of Information Act and National Security Information".

STAT

STAT

OS5-3138

ADMINISTRATIVE - INTERNAL USE ONLY

ADMINISTRATIVE - INTERNAL USE ONLY

3. Both these sections of the regulation apply to all computer storage media to include magnetic tapes, disk packs (both portable and fixed), micrographic media, and the like. Classification and labeling of the media is the responsibility of the owner/creator of that data contained thereon. This would include media currently held in computer centers for processing and storage purposes but which are not owned/created by such centers.

4. It is recognized that immediate and absolute compliance with this interpretation of [ ] may not be practical in some instances. Where such is the case, the affected office is asked to develop a plan of implementation, setting a date for compliance which is mutually agreeable to that office and the Office of Security.

STAT

[ ]

Director of Security

STAT

ADMINISTRATIVE - INTERNAL USE ONLY

UNCLASSIFIED

DCID No. 1/7

## DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/7<sup>1</sup>

### CONTROL OF DISSEMINATION OF FOREIGN INTELLIGENCE

(Effective 5 October 1975)

Pursuant to provisions of Subsection 102(d) of the National Security Act of 1947, as amended, and other authorities vested in the Director of Central Intelligence by the National Security Council, certain controls on dissemination of foreign intelligence and related material<sup>2</sup> (hereafter referred to as foreign intelligence) are hereby established and promulgated.

#### 1. Purpose

This directive establishes certain common controls and procedures for the use and dissemination of foreign intelligence to ensure that, while facilitating the interchange of information for intelligence purposes, there will be adequate protection of foreign intelligence sources and methods. This directive restates applicable portions of National Security Council Directive of 17 May 1972 implementing Executive Order 11652, and prescribes additional controls applicable to the U. S. foreign intelligence mission.

#### 2. Applicability

The controls and procedures set forth in this Directive shall be uniformly applied by all member departments and agencies of the intelligence community in the handling of all materials containing foreign intelligence originated by the Central Intelligence Agency or by the intelligence components of other USIB departments or agencies.

#### 3. National Security Council Directive

a. National Security Council Directive of 17 May 1972 implementing Executive Order 11652 stipulates that, except as otherwise provided by Section 102 of the National Security Act of 1947, classified information or material originating in one department shall not be disseminated outside any other department to which it has been made available without the consent of the originating department. This restriction on dissemination is commonly described as the "third agency rule."

b. The NSC Directive stipulates that the dissemination of classified information, including intelligence and intelligence information, orally, in writing or by any other means, shall be limited to those persons whose official duties or contractual obligations require knowledge or possession thereof. This is commonly referred to as the "need-to-know" principle.

<sup>1</sup> Supersedes DCID 1/7, effective 5 October 1970.

<sup>2</sup> For purposes of this directive, "related material" includes: information describing U. S. foreign intelligence sources and methods, equipment and methodology unique to the acquisition or exploitation of foreign intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from U. S. foreign intelligence collection efforts.

UNCLASSIFIED

c. The NSC Directive also states that documents or portions of documents containing TOP SECRET information shall not be reproduced without the consent of the originating office. All other classified material shall be reproduced sparingly and any stated prohibition against reproduction shall be strictly adhered to.

d. The NSC Directive further requires that the marking, "WARNING NOTICE—SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED," be prominently displayed on all information and materials relating to sensitive intelligence sources and methods; and, that materials so marked will not be disseminated in any manner outside authorized channels without the permission of the originating department and an assessment by the senior intelligence official in the disseminating department as to the potential risk to the national security and to the intelligence sources and methods involved.<sup>3</sup> For special purposes, primarily bibliographic notation, communications, or automatic data processing, this marking may be abbreviated WNINTEL.

#### 4. Advance authorization

a. To facilitate the dissemination and different uses made of classified foreign intelligence within and among USIB departments and agencies, to assure the timely provision of intelligence to consumers and to handle the volume of such materials in a practical way, it is necessary to provide controlled relief to the "third agency rule" within the intelligence community in addition to that provided by Section 102 of the National Security Act of 1947. Accordingly, USIB departments and agencies have been given advance authorization to use each other's classified foreign intelligence in their respective intelligence documents, publications or other information media, and to disseminate their products to third agencies or foreign governments,<sup>4</sup> subject to limitations and procedures prescribed in this Directive.

b. Classified foreign intelligence documents, even though they bear no control markings, will not be released in their original form to third agencies or foreign governments without permission of the originator. Information contained in classified foreign intelligence documents of another department or agency may be extracted or paraphrased and used by the recipient USIB Agency in classified foreign intelligence reports and released to third agencies, except as specifically restricted by control markings prescribed in this directive. For purposes of this authorization, "WARNING NOTICE—SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" shall not be considered a restrictive marking.

<sup>3</sup> Unless otherwise specified by the Director of Central Intelligence in consultation with USIB or as agreed to between originating and recipient agencies, authorized channels include the intelligence components of USIB departments and agencies and within each department and agency (including their contractors and consultants) as determined by the recipient senior intelligence official.

<sup>4</sup> Excepting RESTRICTED DATA and formerly RESTRICTED DATA, which is prohibited from foreign dissemination under Sections 123 and 144 of Public Law 585, Atomic Energy Act of 1954, as amended.

UNCLASSIFIED

UNCLASSIFIED

c. Information contained in classified foreign intelligence documents of another department or agency not bearing any control markings may be extracted or paraphrased and used by the recipient USIB Agency in reports disseminated to foreign governments provided.<sup>4</sup>

(1) No reference is made to the source documents upon which the released product is based.

(2) The source and manner of acquisition of the information are not revealed.

(3) Foreign release is made through established foreign disclosure channels and procedures.

d. Any department or agency disseminating foreign intelligence beyond the departments and agencies of the USIB shall be responsible for ensuring that recipient departments and agencies understand and agree to observe the restrictions prescribed by this directive and maintain adequate safeguards.

e. No release of a classified foreign intelligence document, whether or not bearing a control marking, shall be made to foreign nationals and immigrant aliens, including U. S. Government employed, utilized or integrated foreign nationals and immigrant aliens, without the permission of the originating agency.

5. Additional authorized control markings

a. In addition to the WARNING NOTICE prescribed by NSC Directive any of the following additional markings may be used on foreign intelligence whenever, in the opinion of the originating department or agency, extraordinary circumstances related to the intelligence source or methods require more specific dissemination restrictions. Use of these markings shall be limited to foreign intelligence, the disclosure of which, could: compromise the status of collaborating foreign governments or officials or otherwise seriously damage U. S. relations with foreign governments; subject U. S. citizens or others to the possibility of personal danger or incarceration; seriously impair the continuing cooperation of private individuals providing foreign intelligence; seriously affect the continuing viability of vital technical collection programs; or, result in the possible compromise or loss of some unique foreign intelligence source or method. These control markings will be individually assigned at the time of preparation of the completed document and used in conjunction with classification and other markings required by Executive Order 11652 and the implementing NSC directive and, unless otherwise indicated in 6a below, carried forward to any new format in which that information is incorporated, including oral and visual presentations.

(1) "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR"

This marking shall be used when unique source sensitivity factors, known to the originator, require strict compliance with third agency rule procedures, in addition to a continuing knowledge and supervision on the part of the originator as to the extent to which the original document and information

UNCLASSIFIED

COPY No 664

UNCLASSIFIED

contained therein is disseminated. Documents and information bearing this marking will not be disseminated beyond the Headquarters elements of the recipient organizations and the information contained therein shall not be extracted and incorporated into other reports without the permission of and under conditions prescribed by the originator. (For special purposes, primarily bibliographic notation, communications and automatic data processing, this marking may be abbreviated ORCON.)

(2) "USIB DEPARTMENTS ONLY"

Foreign intelligence so marked will not be disseminated to departments and agencies not represented on the U.S. Intelligence Board without the permission of the originating agency. Within each USIB department and agency dissemination shall be as determined by the recipient senior intelligence official, and may include department or agency contractors and consultants unless specifically prohibited by addition of the "NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS" marking described below. (For special purposes, primarily bibliographic notation, communications and automatic data processing, this marking may be abbreviated USIBONLY.)

(3) "NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS"

Foreign intelligence so marked shall not be disseminated to contractors or contractor consultants without the permission of the originating agency. Examples of when this marking may be used include National Intelligence Estimates and similar national intelligence reports, and other foreign intelligence, which, if disseminated to consultants or contractors, might seriously impair the continuing cooperation of contributing private individuals. This restriction shall not apply to those consultants hired under Civil Service Commission procedures, or comparable procedures derived from authorities vested in heads of departments and agencies by law, and who are normally considered an extension of the office by which they are employed. In applying this control marking, originators will give consideration to the need of USIB member Departments and Agencies to use contractor consultants and contractors to perform services which cannot be adequately performed by U. S. Government personnel. (For special purposes, primarily bibliographic notation, communications, or automatic data processing, this marking may be abbreviated NOCONTRACT.)

(4) "CAUTION—PROPRIETARY INFORMATION INVOLVED"

This marking will be used in conjunction with foreign intelligence obtained from various sources in the U.S. private business sector, and as the information may bear upon proprietary interests of the source, or may otherwise be used to the source's detriment. Recipients of reports bearing this marking shall take every reasonable precaution to ensure that the information is not used to the detriment of the source. This marking may be used in conjunction with the "NOT RELEASABLE TO CONTRACTORS OR CONSULTANTS" marking described above. (For special purposes, primarily bibliographic

UNCLASSIFIED

notation, communication and automatic data processing, this marking may be abbreviated PROPIN.)

**(5) "NOT RELEASABLE TO FOREIGN NATIONALS"**

Foreign Intelligence so marked involves special considerations requiring that it not be released in any form to foreign governments, foreign nationals or non-U.S. citizens without the permission of the originating agency. Examples of when this control marking may be used include: the possible compromise of the status of relations with collaborating foreign governments, or officials; or jeopardizing the continuing viability of vital technical collection programs. (For special purposes, primarily bibliographic notation, communications, or automatic data processing, this marking may be abbreviated NOFORN.) When the originating agency predetermines that information can be released to a specified foreign government(s) the following marking may be used: "THIS INFORMATION HAS BEEN AUTHORIZED FOR RELEASE TO (specified country(s))." (For special purposes, primarily bibliographic notation, communications, or automatic data processing, this marking may be abbreviated "REL (specified countries).")

**6. Procedures governing use of control markings**

a. Any recipient desiring to use foreign intelligence in a manner contrary to the restrictions established by the control markings set forth above shall obtain the permission of the originating agency. Such permission applies only to the specific purpose agreed to by the originator and does not automatically apply to all recipients of the information as originally disseminated unless the originating agency removes the control markings for the benefit of the recipients. In those cases where dissemination outside the recipient agency is desired utilizing lesser or no control markings, the recipient agency should prepare a sanitized version which may be released with the originator's permission.

b. Control markings authorized in paragraphs 3d and 5 above, shall be displayed prominently on documents, incorporated in the text of communication messages, and associated with data stored or processed in automatic data processing systems. Unless the entire document justifies the protection of the control marking(s), each portion requiring the marking(s) shall, to the extent feasible, be marked with the appropriate marking abbreviation authorized by this directive.

c. The standardized restrictions and control markings set forth in this directive are to be employed uniformly by all departments and agencies in the intelligence community, thereby assuring like control and restrictions on the use of foreign intelligence disseminated within the departments and agencies represented on the USIB.

d. The substance of this directive shall be published in appropriate regulatory or notice media of each agency or department, together with appropriate procedures permitting rapid interagency consultation concerning utilization of intelligence and information. For this purpose, each USIB agency will designate a primary referent.

UNCLASSIFIED

COPY NO 664

**UNCLASSIFIED**

**7. Report of unauthorized disclosure**

Violations of the foregoing restrictions and control markings that result in unauthorized disclosure by one agency of the foreign intelligence of another shall be reported to the Director of Central Intelligence through the USIB Security Committee.

**8. Prior restrictions and markings**

Questions with respect to the current application of control markings authorized by earlier directives on the dissemination and control of intelligence and utilized on documents issued prior to the date of this directive should be referred to the originating agency. These markings are: WARNING NOTICE—SENSITIVE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY and NO FOREIGN DISSEM.

W. E. Colby

Director of Central Intelligence



To All Recipients

STAT

STAT

The revised  is in implementation of Executive Order 11652 which became effective on 1 June 1972 and the implementing National Security Council Directive issued May 17, 1972.

STAT

The revised  has been submitted for approval to the Interagency Classification Review Committee as required by the Executive Order. It is issued in the form attached in the interest of having it become effective as soon as possible. It will be reissued in the near future in the normal format of Agency Regulations with any changes required as a result of the review by the Interagency Classification Review Committee. Meanwhile it has the full force and effect of any other Agency Regulation and compliance must begin as soon as possible.

STAT

Supervisors are responsible for the orientation and briefing of employees under their supervision to ensure that they are thoroughly familiar with the provisions  and fully informed of its application. Employees to whom classification authority has been delegated are individually responsible for familiarizing themselves completely with its content.

STAT

Extra copies  may be obtained from the Chief, Regulations Control Branch, Support Services Staff, on extension

STAT

STAT

13 June 1972

NATIONAL SECURITY INFORMATION - CLASSIFICATION,  
DECLASSIFICATION AND ACCESS

STAT

PART I. INTRODUCTION

A. Executive Order 11652 - CIA Implementation. Executive Order 11652 and the implementing National Security Council Directive of May 17, 1972, regulate and control the protection and management of national security information and material and provide for access to such information. This regulation is the Agency implementation of those portions of the foregoing directives which impose requirements with respect to classifying, declassifying and managing, and concerning access to such information. [ ] is the implementation of the provisions of E.O. 11652 concerning storage. [ ] implements the provisions concerning transmission and destruction.

STAT

STAT

B. Purposes - CIA Administration. The primary purpose of the Executive Order and the Directive obviously is to protect information involving national security. An equally important objective is to prevent the system for protecting such information from operating to prevent, unnecessarily or improperly, information from becoming available to the public. To accomplish these objectives, the two directives require the classification of national security information, prohibit its overclassification or classification for improper reasons, and require prompt and orderly declassification when national security considerations permit such action. Physical protection of national security information is required, access to such information is limited, and effective measures to manage such information are required. Agency implementation and administration of the Order will seek to accomplish these objectives. The responsibility of the Director to protect intelligence sources and methods, as prescribed by the National Security Act of 1947, also will be implemented by CIA actions under the Order.

C. Effective Dates. The Executive Order and NSC Directive are effective June 1, 1972. This Revision of [ ] shall become effective upon approval by the Interagency Classification Review Committee.

STAT

D. Definitions. The following definitions are prescribed by E.O. 11652.

1. National Security Information. National security information is information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States.

2. Top Secret. Top Secret refers to that national security information or material which requires the highest degree of protection. The test for assigning Top Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

3. Secret. Secret refers to that national security information or material which requires a substantial degree of protection. The test for assigning Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

4. Confidential. Confidential refers to that national security information or material which requires protection. The test for assigning Confidential classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

**Page Denied**

Next 45 Page(s) In Document Denied

FRIDAY, MARCH 10, 1972

WASHINGTON, D.C.

Volume 37 ■ Number 48

PART II



# THE PRESIDENT

## EXECUTIVE ORDER 11652

Classification and Declassification of  
National Security Information  
and Material

Executive Order

### Title 3—The President

#### EXECUTIVE ORDER 11652

##### Classification and Declassification of National Security Information and Material

The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch.

Within the Federal Government there is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our allies. To protect against actions hostile to the United States, of both an overt and covert nature, it is essential that such official information and material be given only limited dissemination.

This official information or material, referred to as classified information or material in this order, is expressly exempted from public disclosure by Section 552(b)(1) of Title 5, United States Code. Wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution.

To ensure that such information and material is protected, but only to the extent and for such period as is necessary, this order identifies the information to be protected, prescribes classification, downgrading, declassification and safeguarding procedures to be followed, and establishes a monitoring system to ensure its effectiveness.

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, it is hereby ordered:

**SECTION 1. *Security Classification Categories.*** Official information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (hereinafter collectively termed "national security") shall be classified in one of three categories, namely "Top Secret," "Secret," or "Confidential," depending upon the degree of its significance to national security. No other categories shall be used to identify official information or material as requiring protection in the interest of national security, except as otherwise expressly provided by statute. These classification categories are defined as follows:

(A) "*Top Secret.*" "Top Secret" refers to that national security information or material which requires the highest degree of protection. The test for assigning "Top Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the

## THE PRESIDENT

national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with the utmost restraint.

(B) "*Secret*." "Secret" refers to that national security information or material which requires a substantial degree of protection. The test for assigning "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. The classification "Secret" shall be sparingly used.

(C) "*Confidential*." "Confidential" refers to that national security information or material which requires protection. The test for assigning "Confidential" classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

SEC. 2. *Authority to Classify*. The authority to originally classify information or material under this order shall be restricted solely to those offices within the executive branch which are concerned with matters of national security, and shall be limited to the minimum number absolutely required for efficient administration. Except as the context may otherwise indicate, the term "Department" as used in this order shall include agency or other governmental unit.

(A) The authority to originally classify information or material under this order as "Top Secret" shall be exercised only by such officials as the President may designate in writing and by:

- (1) The heads of the Departments listed below;
- (2) Such of their senior principal deputies and assistants as the heads of such Departments may designate in writing; and
- (3) Such heads and senior principal deputies and assistants of major elements of such Departments, as the heads of such Departments may designate in writing.

Such offices in the Executive Office of the President as the President may designate in writing

Central Intelligence Agency  
Atomic Energy Commission  
Department of State  
Department of the Treasury  
Department of Defense  
Department of the Army  
Department of the Navy  
Department of the Air Force  
United States Arms Control and Disarmament Agency

Department of Justice  
National Aeronautics and Space Administration  
Agency for International Development

(B) The authority to originally classify information or material under this order as "Secret" shall be exercised only by:

- (1) Officials who have "Top Secret" classification authority;
- (2) Such subordinates as officials with "Top Secret" classification authority under (A) (1) and (2) above may designate in writing; and
- (3) The heads of the following named Departments and such senior principal deputies or assistants as they may designate in writing.

Department of Transportation  
Federal Communications Commission  
Export-Import Bank of the United States  
Department of Commerce  
United States Civil Service Commission  
United States Information Agency  
General Services Administration  
Department of Health, Education, and Welfare  
Civil Aeronautics Board  
Federal Maritime Commission  
Federal Power Commission  
National Science Foundation  
Overseas Private Investment Corporation

(C) The authority to originally classify information or material under this order as "Confidential" may be exercised by officials who have "Top Secret" or "Secret" classification authority and such officials as they may designate in writing.

(D) Any Department not referred to herein and any Department or unit established hereafter shall not have authority to originally classify information or material under this order, unless specifically authorized hereafter by an Executive order.

SEC. 3. *Authority to Downgrade and Declassify.* The authority to downgrade and declassify national security information or material shall be exercised as follows:

(A) Information or material may be downgraded or declassified by the official authorizing the original classification, by a successor in capacity or by a supervisory official of either.

(B) Downgrading and declassification authority may also be exercised by an official specifically authorized under regulations issued by the head of the Department listed in Sections 2(A) or (B) hereof.

(C) In the case of classified information or material officially transferred by or pursuant to statute or Executive order in conjunction with a transfer of function and not merely for storage purposes, the receiving Department shall be deemed to be the originating Department for all purposes under this order including downgrading and declassification.



(D) In the case of classified information or material not officially transferred within (C) above, but originated in a Department which has since ceased to exist, each Department in possession shall be deemed to be the originating Department for all purposes under this order. Such information or material may be downgraded and declassified by the Department in possession after consulting with any other Departments having an interest in the subject matter.

(E) Classified information or material transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded and declassified by the Archivist of the United States in accordance with this order, directives of the President issued through the National Security Council and pertinent regulations of the Departments.

(F) Classified information or material with special markings, as described in Section 8, shall be downgraded and declassified as required by law and governing regulations.

SEC. 4. *Classification.* Each person possessing classifying authority shall be held accountable for the propriety of the classifications attributed to him. Both unnecessary classification and over-classification shall be avoided. Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security. The following rules shall apply to classification of information under this order:

(A) *Documents in General.* Each classified document shall show on its face its classification and whether it is subject to or exempt from the General Declassification Schedule. It shall also show the office of origin, the date of preparation and classification and, to the extent practicable, be so marked as to indicate which portions are classified, at what level, and which portions are not classified in order to facilitate excerpting and other use. Material containing references to classified materials, which references do not reveal classified information, shall not be classified.

(B) *Identification of Classifying Authority.* Unless the Department involved shall have provided some other method of identifying the individual at the highest level that authorized classification in each case, material classified under this order shall indicate on its face the identity of the highest authority authorizing the classification. Where the individual who signs or otherwise authenticates a document or item has also authorized the classification, no further annotation as to his identity is required.

(C) *Information or Material Furnished by a Foreign Government or International Organization.* Classified information or material furnished to the United States by a foreign government or international organization shall either retain its original classification or be assigned a United States classification. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information or material.

(D) *Classification Responsibilities.* A holder of classified information or material shall observe and respect the classification assigned by the originator. If a holder believes that there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification under this order, he shall so inform the originator who shall thereupon re-examine the classification.

SEC. 5. *Declassification and Downgrading.* Classified information and material, unless declassified earlier by the original classifying authority, shall be declassified and downgraded in accordance with the following rules:

(A) *General Declassification Schedule.* (1) "Top Secret." Information or material originally classified "Top Secret" shall become automatically downgraded to "Secret" at the end of the second full calendar year following the year in which it was originated, downgraded to "Confidential" at the end of the fourth full calendar year following the year in which it was originated, and declassified at the end of the tenth full calendar year following the year in which it was originated.

(2) "Secret." Information and material originally classified "Secret" shall become automatically downgraded to "Confidential" at the end of the second full calendar year following the year in which it was originated, and declassified at the end of the eighth full calendar year following the year in which it was originated.

(3) "Confidential." Information and material originally classified "Confidential" shall become automatically declassified at the end of the sixth full calendar year following the year in which it was originated.

(B) *Exemptions from General Declassification Schedule.* Certain classified information or material may warrant some degree of protection for a period exceeding that provided in the General Declassification Schedule. An official authorized to originally classify information or material "Top Secret" may exempt from the General Declassification Schedule any level of classified information or material originated by him or under his supervision if it falls within one of the categories described below. In each case such official shall specify in writing on the material the exemption category being claimed and, unless impossible, a date or event for automatic declassification. The use of the exemption authority shall be kept to the absolute minimum consistent with national security requirements and shall be restricted to the following categories:

(1) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.

(2) Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

(3) Classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security.

(4) Classified information or material the disclosure of which would place a person in immediate jeopardy.

(C) *Mandatory Review of Exempted Material.* All classified information and material originated after the effective date of this order which is exempted under (B) above from the General Declassification Schedule shall be subject to a classification review by the originating Department at any time after the expiration of ten years from the date of origin provided:

(1) A Department or member of the public requests a review;

(2) The request describes the record with sufficient particularity to enable the Department to identify it; and

(3) The record can be obtained with only a reasonable amount of effort.

Information or material which no longer qualifies for exemption under (B) above shall be declassified. Information or material continuing to qualify under (B) shall be so marked and, unless impossible, a date for automatic declassification shall be set.

(D) *Applicability of the General Declassification Schedule to Previously Classified Material.* Information or material classified before the effective date of this order and which is assigned to Group 4 under Executive Order No. 10501, as amended by Executive Order No. 10964, shall be subject to the General Declassification Schedule. All other information or material classified before the effective date of this order, whether or not assigned to Groups 1, 2, or 3 of Executive Order No. 10501, as amended, shall be excluded from the General Declassification Schedule. However, at any time after the expiration of ten years from the date of origin it shall be subject to a mandatory classification review and disposition under the same conditions and criteria that apply to classified information and material created after the effective date of this order as set forth in (B) and (C) above.

(E) *Declassification of Classified Information or Material After Thirty Years.* All classified information or material which is thirty years old or more, whether originating before or after the effective date of this order, shall be declassified under the following conditions:

(1) All information and material classified after the effective date of this order shall, whether or not declassification has been requested, become automatically declassified at the end of thirty full calendar years after the date of its original classification except for such specifically identified information or material which the head of the originating Department personally determines in writing at that time to require continued protection because such continued protection is essential to the national security or disclosure would place a person in immediate jeopardy. In such case, the head of the Department shall also specify the period of continued classification.

(2) All information and material classified before the effective date of this order and more than thirty years old shall be systematically reviewed for declassification by the Archivist of the United States by the end of the thirtieth full calendar year following the year in which it was

Approved For Release 2007/07/10 : CIA-RDP86-00674R000200120002-6

originated. In his review, the Archivist will separate and keep protected only such information or material as is specifically identified by the head of the Department in accordance with (E)(1) above. In such case, the head of the Department shall also specify the period of continued classification.

(F) *Departments Which Do Not Have Authority For Original Classification.* The provisions of this section relating to the declassification of national security information or material shall apply to Departments which, under the terms of this order, do not have current authority to originally classify information or material, but which formerly had such authority under previous Executive orders.

SEC. 6. *Policy Directives on Access, Marking, Safekeeping, Accountability, Transmission, Disposition and Destruction of Classified Information and Material.* The President acting through the National Security Council shall issue directives which shall be binding on all Departments to protect classified information from loss or compromise. Such directives shall conform to the following policies:

(A) No person shall be given access to classified information or material unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of his duties.

(B) All classified information and material shall be appropriately and conspicuously marked to put all persons on clear notice of its classified contents.

(C) Classified information and material shall be used, possessed, and stored only under conditions which will prevent access by unauthorized persons or dissemination to unauthorized persons.

(D) All classified information and material disseminated outside the executive branch under Executive Order No. 10865 or otherwise shall be properly protected.

(E) Appropriate accountability records for classified information shall be established and maintained and such information and material shall be protected adequately during all transmissions.

(F) Classified information and material no longer needed in current working files or for reference or record purposes shall be destroyed or disposed of in accordance with the records disposal provisions contained in Chapter 33 of Title 44 of the United States Code and other applicable statutes.

(G) Classified information or material shall be reviewed on a systematic basis for the purpose of accomplishing downgrading, declassification, transfer, retirement and destruction at the earliest practicable date.

SEC. 7. *Implementation and Review Responsibilities.* (A) The National Security Council shall monitor the implementation of this order. To assist the National Security Council, an Interagency Classification Review Committee shall be established, composed of representatives of the Departments of State, Defense and Justice, the Atomic Energy Commission, the Central Intelligence Agency and the National

Security Council Staff and a Chairman designated by the President. Representatives of other Departments in the executive branch may be invited to meet with the Committee on matters of particular interest to those Departments. This Committee shall meet regularly and on a continuing basis shall review and take action to ensure compliance with this order, and in particular:

(1) The Committee shall oversee Department actions to ensure compliance with the provisions of this order and implementing directives issued by the President through the National Security Council.

(2) The Committee shall, subject to procedures to be established by it, receive, consider and take action on suggestions and complaints from persons within or without the government with respect to the administration of this order, and in consultation with the affected Department or Departments assure that appropriate action is taken on such suggestions and complaints.

(3) Upon request of the Committee Chairman, any Department shall furnish to the Committee any particular information or material needed by the Committee in carrying out its functions.

(B) To promote the basic purposes of this order, the head of each Department originating or handling classified information or material shall:

(1) Prior to the effective date of this order submit to the Interagency Classification Review Committee for approval a copy of the regulations it proposes to adopt pursuant to this order.

(2) Designate a senior member of his staff who shall ensure effective compliance with and implementation of this order and shall also chair a Departmental committee which shall have authority to act on all suggestions and complaints with respect to the Department's administration of this order.

(3) Undertake an initial program to familiarize the employees of his Department with the provisions of this order. He shall also establish and maintain active training and orientation programs for employees concerned with classified information or material. Such programs shall include, as a minimum, the briefing of new employees and periodic reorientation during employment to impress upon each individual his responsibility for exercising vigilance and care in complying with the provisions of this order. Additionally, upon termination of employment or contemplated temporary separation for a sixty-day period or more, employees shall be debriefed and each reminded of the provisions of the Criminal Code and other applicable provisions of law relating to penalties for unauthorized disclosure.

(C) The Attorney General, upon request of the head of a Department, his duly designated representative, or the Chairman of the above described Committee, shall personally or through authorized representatives of the Department of Justice render an interpretation of this order with respect to any question arising in the course of its administration.

SEC. 8. *Material Covered by the Atomic Energy Act.* Nothing in this order shall supersede any requirements made by or under the Atomic Energy Act of August 30, 1954, as amended. "Restricted Data," and material designated as "Formerly Restricted Data," shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and the regulations of the Atomic Energy Commission.

SEC. 9. *Special Departmental Arrangements.* The originating Department or other appropriate authority may impose, in conformity with the provisions of this order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography.

SEC. 10. *Exceptional Cases.* In an exceptional case when a person or Department not authorized to classify information originates information which is believed to require classification, such person or Department shall protect that information in the manner prescribed by this order. Such persons or Department shall transmit the information forthwith, under appropriate safeguards, to the Department having primary interest in the subject matter with a request that a determination be made as to classification.

SEC. 11. *Declassification of Presidential Papers.* The Archivist of the United States shall have authority to review and declassify information and material which has been classified by a President, his White House Staff or special committee or commission appointed by him and which the Archivist has in his custody at any archival depository, including a Presidential Library. Such declassification shall only be undertaken in accord with: (i) the terms of the donor's deed of gift, (ii) consultations with the Departments having a primary subject-matter interest, and (iii) the provisions of Section 5.

SEC. 12. *Historical Research and Access by Former Government Officials.* The requirement in Section 6(A) that access to classified information or material be granted only as is necessary for the performance of one's duties shall not apply to persons outside the executive branch who are engaged in historical research projects or who have previously occupied policy-making positions to which they were appointed by the President; *Provided*, however, that in each case the head of the originating Department shall:

(i) determine that access is clearly consistent with the interests of national security; and

(ii) take appropriate steps to assure that classified information or material is not published or otherwise compromised.

Access granted a person by reason of his having previously occupied a policy-making position shall be limited to those papers which the former official originated, reviewed, signed or received while in public office.


SEC. 13. *Administrative and Judicial Action.* (A) Any officer or employee of the United States who unnecessarily classifies or over-

classifies information or material shall be notified that his actions are in violation of the terms of this order or of a directive of the President issued through the National Security Council. Repeated abuse of the classification process shall be grounds for an administrative reprimand. In any case where the Departmental committee or the Interagency Classification Review Committee finds that unnecessary classification or overclassification has occurred, it shall make a report to the head of the Department concerned in order that corrective steps may be taken.

(B) The head of each Department is directed to take prompt and stringent administrative action against any officer or employee of the United States, at any level of employment, determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by or under this order or a directive of the President issued through the National Security Council. Where a violation of criminal statutes may be involved, Departments will refer any such case promptly to the Department of Justice.

SEC. 14. *Revocation of Executive Order No. 10501.* Executive Order No. 10501 of November 5, 1953, as amended by Executive Orders No. 10816 of May 8, 1959, No. 10901 of January 11, 1961, No. 10964 of September 20, 1961, No. 10985 of January 15, 1962, No. 11097 of March 6, 1963 and by Section 1(a) of No. 11382 of November 28, 1967, is superseded as of the effective date of this order.

SEC. 15. *Effective date.* This order shall become effective on June 1, 1972.



THE WHITE HOUSE,  
March 8, 1972.

[FR Doc.72-3782 Filed 3-9-72; 11:01 am]

SECURITY

STAT

CLASSIFICATION AND DECLASSIFICATION  
OF NATIONAL SECURITY INFORMATION

DISTRIBUTION: AB



FOREWORD

STAT

FOREWORD

This handbook explains and amplifies the policies contained  
in  concerning classification and declassification of  
National Security Information and prescribes detailed implementing  
instructions for the procedures contained therein.

STAT

FOR THE DIRECTOR OF CENTRAL INTELLIGENCE:

JOHN W. COFFEY  
Deputy Director  
for Support

DISTRIBUTION: AB

SECURITY

  
 CONTENTS

STAT

## CONTENTS

## CHAPTER 1: GENERAL CONSIDERATIONS

| <u>Paragraph</u>   | <u>Page</u> |
|--|-------------|
| 1. BASIC POLICY . . . . .  |             |
| 2. EXECUTIVE ORDER 11652 . . . . .   |             |
| 3. APPLICABILITY TO THIS AGENCY . . . . .  |             |
| 4. OTHER APPLICABLE LAWS AND REGULATIONS . . . . .   |             |
| 5. INDIVIDUAL RESPONSIBILITY . . . . .   |             |
| 6. ELECTRICAL TRANSMISSIONS, COMPUTER OUTPUT, MICROFILM, AND<br>OTHER MEDIA . . . . .                |             |
| 7. METHODS BY WHICH INFORMATION MAY BE PROTECTED . . . . .   |             |
| a. CLASSIFICATION . . . . .  |             |
| b. PRIVILEGED INFORMATION . . . . .  |             |
| c. SPECIAL PROTECTIVE MEASURES, COMPARTMENTATION SYSTEMS,<br>AND DISSEMINATION CONTROLS . . . . .    |             |
| d. SECURE HANDLING . . . . .   |             |
| 8. PROCEDURE TO CLASSIFY OR CORRECT THE CLASSIFICATION OF<br>NATIONAL SECURITY INFORMATION . . . . . |             |
| 9. PROCEDURE TO EXEMPT INFORMATION FROM THE GENERAL<br>DECLASSIFICATION SCHEDULE . . . . .           |             |

## CHAPTER 2: REQUIRED RECORDS

|  |  |
|--|--|
| 10. AUTHORITY TO CLASSIFY . . . . .  |  |
| 11. DELEGATION OF NATIONAL SECURITY CLASSIFICATION AUTHORITY . .                           |  |
| 12. SPECIFIC PROCEDURE TO DELEGATE NATIONAL SECURITY<br>CLASSIFICATION AUTHORITY . . . . . |  |
| 13. IDENTIFICATION OF CLASSIFIER . . . . .   |  |

## CHAPTER 3: DOWNGRADING AND DECLASSIFICATION

|  |  |
|--|--|
| 14. GENERAL POLICY AND CAVEATS . . . . .   |  |
| 15. ACTIONS REQUIRED TO PREVENT INADVERTENT DISCLOSURE OF<br>SENSITIVE INFORMATION . . . . . |  |
| 16. PROCEDURE TO DOWNGRADE OR DECLASSIFY NATIONAL SECURITY<br>INFORMATION . . . . .          |  |

## CHAPTER 4: MARKINGS AND STAMPS

|                                     |  |
|-------------------------------------|--|
| 17. GENERAL REQUIREMENTS . . . . .  |  |
| 18. SPECIFIC REQUIREMENTS . . . . . |  |



SECURITY

STAT

CONTENTS

| <u>Paragraph</u>  | <u>Page</u> |
|---|-------------|
| a. SECURITY CLASSIFICATION CATEGORY -- TOP SECRET, SECRET, AND CONFIDENTIAL . . . . . |             |
| b. CLASSIFIED BY - GENERAL DECLASSIFICATION SCHEDULE MARKINGS . . . . .               |             |
| c. WARNING NOTICES . . . . .  |             |
| d. ATOMIC ENERGY INFORMATION . . . . .  |             |
| e. INFORMATION FURNISHED OUTSIDE THE EXECUTIVE BRANCH . .                             |             |
| f. SENSITIVE INTELLIGENCE . . . . .   |             |
| g. ADMINISTRATIVE NOTICES . . . . .   |             |
| 19. PRINTED FORMS . . . . .   |             |
| 20. REMARKING DOWNGRADED OR DECLASSIFIED INFORMATION AND MATERIAL . . . . .           |             |

**Page Denied**

Next 43 Page(s) In Document Denied

March 8, 1972

Office of the White House Press Secretary

---

THE WHITE HOUSE

## EXECUTIVE ORDER

---

CLASSIFICATION AND DECLASSIFICATION OF NATIONAL  
SECURITY INFORMATION AND MATERIAL

The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch.

Within the Federal Government there is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our allies. To protect against actions hostile to the United States, of both an overt and covert nature, it is essential that such official information and material be given only limited dissemination.

This official information or material, referred to as classified information or material in this order, is expressly exempted from public disclosure by Section 552(b)(1) of Title 5, United States Code. Wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution.

To ensure that such information and material is protected, but only to the extent and for such period as is necessary, this order identifies the information to be protected, prescribes classification, downgrading, declassification and safeguarding procedures to be followed, and establishes a monitoring system to ensure its effectiveness.

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, it is hereby ordered:

Section 1. Security Classification Categories. Official information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (hereinafter collectively termed "national security") shall be classified in one of three categories, namely "Top Secret," "Secret," or "Confidential," depending upon the degree of its significance to national security. No other categories shall be used to identify official information or material as requiring protection in the interest of national security, except as otherwise expressly provided by statute. These classification categories are defined as follows:

(A) "Top Secret." "Top Secret" refers to that national security information or material which requires the highest degree of protection. The test for assigning "Top Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed

more

hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with the utmost restraint.

(B) "Secret." "Secret" refers to that national security information or material which requires a substantial degree of protection. The test for assigning "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. The classification "Secret" shall be sparingly used.

(C) "Confidential." "Confidential" refers to that national security information or material which requires protection. The test for assigning "Confidential" classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

Section 2. Authority to Classify. The authority to originally classify information or material under this order shall be restricted solely to those offices within the executive branch which are concerned with matters of national security, and shall be limited to the minimum number absolutely required for efficient administration. Except as the context may otherwise indicate, the term "Department" as used in this order shall include agency or other governmental unit.

(A) The authority to originally classify information or material under this order as "Top Secret" shall be exercised only by such officials as the President may designate in writing and by:

- (1) The heads of the Departments listed below;
- (2) Such of their senior principal deputies and assistants as the heads of such Departments may designate in writing; and
- (3) Such heads and senior principal deputies and assistants of major elements of such Departments, as the heads of such Departments may designate in writing.

Such offices in the Executive Office of the President as the President may designate in writing

Central Intelligence Agency  
Atomic Energy Commission  
Department of State  
Department of the Treasury  
Department of Defense  
Department of the Army  
Department of the Navy  
Department of the Air Force  
United States Arms Control and Disarmament Agency  
Department of Justice  
National Aeronautics and Space Administration  
Agency for International Development

more

(B) The authority to originally classify information or material under this order as "Secret" shall be exercised only by:

- (1) Officials who have "Top Secret" classification authority;
- (2) Such subordinates as officials with "Top Secret" classification authority under (A)(1) and (2) above may designate in writing; and
- (3) The heads of the following named Departments and such senior principal deputies or assistants as they may designate in writing.

Department of Transportation  
 Federal Communications Commission  
 Export-Import Bank of the United States  
 Department of Commerce  
 United States Civil Service Commission  
 United States Information Agency  
 General Services Administration  
 Department of Health, Education, and Welfare  
 Civil Aeronautics Board  
 Federal Maritime Commission  
 Federal Power Commission  
 National Science Foundation  
 Overseas Private Investment Corporation

(C) The authority to originally classify information or material under this order as "Confidential" may be exercised by officials who have "Top Secret" or "Secret" classification authority and such officials as they may designate in writing.

(D) Any Department not referred to herein and any Department or unit established hereafter shall not have authority to originally classify information or material under this order, unless specifically authorized hereafter by an Executive order.

Section 3. Authority to Downgrade and Declassify. The authority to downgrade and declassify national security information or material shall be exercised as follows:

(A) Information or material may be downgraded or declassified by the official authorizing the original classification, by a successor in capacity or by a supervisory official of either.

(B) Downgrading and declassification authority may also be exercised by an official specifically authorized under regulations issued by the head of the Department listed in Sections 2(A) or (B) hereof.

(C) In the case of classified information or material officially transferred by or pursuant to statute or Executive order in conjunction with a transfer of function and not merely for storage purposes, the receiving Department shall be deemed to be the originating Department for all purposes under this order including downgrading and declassification.

(D) In the case of classified information or material not officially transferred within (C) above, but originated in a Department which has since ceased to exist, each Department in possession shall be deemed to be the originating Department for all purposes under this order.

more

Such information or material may be downgraded and declassified by the Department in possession after consulting with any other Departments having an interest in the subject matter.

(E) Classified information or material transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded and declassified by the Archivist of the United States in accordance with this order, directives of the President issued through the National Security Council and pertinent regulations of the Departments.

(F) Classified information or material with special markings, as described in Section 8, shall be downgraded and declassified as required by law and governing regulations.

Section 4. Classification. Each person possessing classifying authority shall be held accountable for the propriety of the classifications attributed to him. Both unnecessary classification and over-classification shall be avoided. Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security. The following rules shall apply to classification of information under this order:

(A) Documents in General. Each classified document shall show on its face its classification and whether it is subject to or exempt from the General Declassification Schedule. It shall also show the office of origin, the date of preparation and classification and, to the extent practicable, be so marked as to indicate which portions are classified, at what level, and which portions are not classified in order to facilitate excerpting and other use. Material containing references to classified materials, which references do not reveal classified information, shall not be classified.

(B) Identification of Classifying Authority. Unless the Department involved shall have provided some other method of identifying the individual at the highest level that authorized classification in each case, material classified under this order shall indicate on its face the identity of the highest authority authorizing the classification. Where the individual who signs or otherwise authenticates a document or item has also authorized the classification, no further annotation as to his identity is required.

(C) Information or Material Furnished by a Foreign Government or International Organization. Classified information or material furnished to the United States by a foreign government or international organization shall either retain its original classification or be assigned a United States classification. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information or material.

(D) Classification Responsibilities. A holder of classified information or material shall observe and respect the classification assigned by the originator. If a holder believes that there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification under

more



this order, he shall so inform the originator who shall thereupon re-examine the classification.

Section 5. Declassification and Downgrading. Classified information and material, unless declassified earlier by the original classifying authority, shall be declassified and downgraded in accordance with the following rules:

(A) General Declassification Schedule.

(1) "Top Secret." Information or material originally classified "Top Secret" shall become automatically downgraded to "Secret" at the end of the second full calendar year following the year in which it was originated, downgraded to "Confidential" at the end of the fourth full calendar year following the year in which it was originated, and declassified at the end of the tenth full calendar year following the year in which it was originated.

(2) "Secret." Information and material originally classified "Secret" shall become automatically downgraded to "Confidential" at the end of the second full calendar year following the year in which it was originated, and declassified at the end of the eighth full calendar year following the year in which it was originated.

(3) "Confidential." Information and material originally classified "Confidential" shall become automatically declassified at the end of the sixth full calendar year following the year in which it was originated.

(B) Exemptions from General Declassification Schedule. Certain classified information or material may warrant some degree of protection for a period exceeding that provided in the General Declassification Schedule. An official authorized to originally classify information or material "Top Secret" may exempt from the General Declassification Schedule any level of classified information or material originated by him or under his supervision if it falls within one of the categories described below. In each case such official shall specify in writing on the material the exemption category being claimed and, unless impossible, a date or event for automatic declassification. The use of the exemption authority shall be kept to the absolute minimum consistent with national security requirements and shall be restricted to the following categories:

(1) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.

(2) Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

(3) Classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security.

(4) Classified information or material the disclosure of which would place a person in immediate jeopardy.

more

(C) Mandatory Review of Exempted Material. All classified information and material originated after the effective date of this order which is exempted under (B) above from the General Declassification Schedule shall be subject to a classification review by the originating Department at any time after the expiration of ten years from the date of origin provided:

- (1) A Department or member of the public requests a review;
- (2) The request describes the record with sufficient particularity to enable the Department to identify it; and
- (3) The record can be obtained with only a reasonable amount of effort.

Information or material which no longer qualifies for exemption under (B) above shall be declassified. Information or material continuing to qualify under (B) shall be so marked and, unless impossible, a date for automatic declassification shall be set.

(D) Applicability of the General Declassification Schedule to Previously Classified Material. Information or material classified before the effective date of this order and which is assigned to Group 4 under Executive Order No. 10501, as amended by Executive Order No. 10964, shall be subject to the General Declassification Schedule. All other information or material classified before the effective date of this order, whether or not assigned to Groups 1, 2, or 3 of Executive Order No. 10501, as amended, shall be excluded from the General Declassification Schedule. However, at any time after the expiration of ten years from the date of origin it shall be subject to a mandatory classification review and disposition under the same conditions and criteria that apply to classified information and material created after the effective date of this order as set forth in (B) and (C) above.

(E) Declassification of Classified Information or Material After Thirty Years. All classified information or material which is thirty years old or more, whether originating before or after the effective date of this order, shall be declassified under the following conditions:

- (1) All information and material classified after the effective date of this order shall, whether or not declassification has been requested, become automatically declassified at the end of thirty full calendar years after the date of its original classification except for such specifically identified information or material which the head of the originating Department personally determines in writing at that time to require continued protection because such continued protection is essential to the national security or disclosure would place a person in immediate jeopardy. In such case, the head of the Department shall also specify the period of continued classification.
- (2) All information and material classified before the effective date of this order and more than thirty years old shall be systematically reviewed for declassification by the Archivist of the United States by the end of the thirtieth full calendar year following the year in which it was originated. In his review, the Archivist will separate and keep protected

more

25X1

only such information or material as is specifically identified by the head of the Department in accordance with (E)(1) above. In such case, the head of the Department shall also specify the period of continued classification.

(F) Departments Which Do Not Have Authority For Original Classification. The provisions of this section relating to the declassification of national security information or material shall apply to Departments which, under the terms of this order, do not have current authority to originally classify information or material, but which formerly had such authority under previous Executive orders.

Section 6. Policy Directives on Access, Marking, Safekeeping, Accountability, Transmission, Disposition and Destruction of Classified Information and Material. The President acting through the National Security Council shall issue directives which shall be binding on all Departments to protect classified information from loss or compromise. Such directives shall conform to the following policies:

- (A) No person shall be given access to classified information or material unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of his duties.
- (B) All classified information and material shall be appropriately and conspicuously marked to put all persons on clear notice of its classified contents.
- (C) Classified information and material shall be used, possessed, and stored only under conditions which will prevent access by unauthorized persons or dissemination to unauthorized persons.
- (D) All classified information and material disseminated outside the executive branch under Executive Order No. 10865 or otherwise shall be properly protected.
- (E) Appropriate accountability records for classified information shall be established and maintained and such information and material shall be protected adequately during all transmissions.
- (F) Classified information and material no longer needed in current working files or for reference or record purposes shall be destroyed or disposed of in accordance with the records disposal provisions contained in Chapter 33 of Title 44 of the United States Code and other applicable statutes.
- (G) Classified information or material shall be reviewed on a systematic basis for the purpose of accomplishing downgrading, declassification, transfer, retirement and destruction at the earliest practicable date.

Section 7. Implementation and Review Responsibilities.

(A) The National Security Council shall monitor the implementation of this order. To assist the National Security Council, an Interagency Classification Review Committee shall be established, composed of representatives of the Departments of State, Defense and Justice, the Atomic Energy Commission, the Central Intelligence Agency and the National Security Council Staff and a Chairman designated by the President. Representatives of other Departments in the executive branch may be invited to

more

meet with the Committee on matters of particular interest to those Departments. This Committee shall meet regularly and on a continuing basis shall review and take action to ensure compliance with this order, and in particular:

(1) The Committee shall oversee Department actions to ensure compliance with the provisions of this order and implementing directives issued by the President through the National Security Council.

(2) The Committee shall, subject to procedures to be established by it, receive, consider and take action on suggestions and complaints from persons within or without the government with respect to the administration of this order, and in consultation with the affected Department or Departments assure that appropriate action is taken on such suggestions and complaints.

(3) Upon request of the Committee Chairman, any Department shall furnish to the Committee any particular information or material needed by the Committee in carrying out its functions.

(B) To promote the basic purposes of this order, the head of each Department originating or handling classified information or material shall:

(1) Prior to the effective date of this order submit to the Interagency Classification Review Committee for approval a copy of the regulations it proposes to adopt pursuant to this order.

(2) Designate a senior member of his staff who shall ensure effective compliance with and implementation of this order and shall also chair a Departmental committee which shall have authority to act on all suggestions and complaints with respect to the Department's administration of this order.

(3) Undertake an initial program to familiarize the employees of his Department with the provisions of this order. He shall also establish and maintain active training and orientation programs for employees concerned with classified information or material. Such programs shall include, as a minimum, the briefing of new employees and periodic reorientation during employment to impress upon each individual his responsibility for exercising vigilance and care in complying with the provisions of this order. Additionally, upon termination of employment or contemplated temporary separation for a sixty-day period or more, employees shall be debriefed and each reminded of the provisions of the Criminal Code and other applicable provisions of law relating to penalties for unauthorized disclosure.

(C) The Attorney General, upon request of the head of a Department, his duly designated representative, or the Chairman of the above described Committee, shall personally or through authorized representatives of the Department of Justice render an interpretation of this order with respect to any question arising in the course its administration.

more

Section 8. Material Covered by the Atomic Energy Act. Nothing in this order shall supersede any requirements made by or under the Atomic Energy Act of August 30, 1954, as amended. "Restricted Data," and material designated as "Formerly Restricted Data," shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and the regulations of the Atomic Energy Commission.

Section 9. Special Departmental Arrangements. The originating Department or other appropriate authority may impose, in conformity with the provisions of this order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography.

Section 10. Exceptional Cases. In an exceptional case when a person or Department not authorized to classify information originates information which is believed to require classification, such person or Department shall protect that information in the manner prescribed by this order. Such persons or Department shall transmit the information forthwith, under appropriate safeguards, to the Department having primary interest in the subject matter with a request that a determination be made as to classification.

Section 11. Declassification of Presidential Papers. The Archivist of the United States shall have authority to review and declassify information and material which has been classified by a President, his White House Staff or special committee or commission appointed by him and which the Archivist has in his custody at any archival depository, including a Presidential Library. Such declassification shall only be undertaken in accord with: (i) the terms of the donor's deed of gift, (ii) consultations with the Departments having a primary subject-matter interest, and (iii) the provisions of Section 5.

Section 12. Historical Research and Access by Former Government Officials. The requirement in Section 6(A) that access to classified information or material be granted only as is necessary for the performance of one's duties shall not apply to persons outside the executive branch who are engaged in historical research projects or who have previously occupied policy-making positions to which they were appointed by the President; Provided, however, that in each case the head of the originating Department shall:

(i) determine that access is clearly consistent with the interests of national security; and

(ii) take appropriate steps to assure that classified information or material is not published or otherwise compromised.

Access granted a person by reason of his having previously occupied a policy-making position shall be limited to those papers which the former official originated, reviewed, signed or received while in public office.

Section 13. Administrative and Judicial Action.

(A) Any officer or employee of the United States who unnecessarily classifies or over-classifies information

more

10

or material shall be notified that his actions are in violation of the terms of this order or of a directive of the President issued through the National Security Council. Repeated abuse of the classification process shall be grounds for an administrative reprimand. In any case where the Departmental committee or the Inter-agency Classification Review Committee finds that unnecessary classification or over-classification has occurred, it shall make a report to the head of the Department concerned in order that corrective steps may be taken.

(B) The head of each Department is directed to take prompt and stringent administrative action against any officer or employee of the United States, at any level of employment, determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by or under this order or a directive of the President issued through the National Security Council. Where a violation of criminal statutes may be involved, Departments will refer any such case promptly to the Department of Justice.

Section 14. Revocation of Executive Order No. 10501. Executive Order No. 10501 of November 5, 1953, as amended by Executive Orders No. 10816 of May 8, 1959, No. 10901 of January 11, 1961, No. 10964 of September 20, 1961, No. 10985 of January 15, 1962, No. 11097 of March 6, 1963 and by Section 1(a) of No. 11382 of November 28, 1967, are superseded as of the effective date of this order.

Section 15. Effective Date. This order shall become effective on June 1, 1972.

RICHARD NIXON

THE WHITE HOUSE,

# # # # #